(12) UK Patent Application (19) GB (11) 2 281 648 (13) A

(43) Date of A Publication 08.03.1995

(21) Application No 9417777.1

(22) Date of Filing 05.09.1994

(30) Priority Data
(31) 930648 (32) 06.09.1993 (33) IE

(71) Applicant(s)
Turquoise holdings Limited

(Incorporated in Ireland)

Station Road, KILLINEY, County Dublin, Ireland

(72) Inventor(s)
Patrick Shiel
John Clarke

(74) Agent and/or Address for Service
E Eder & Co
39 Cranbrook Road, ILFORD, Essex, IG1 4PA,
United Kingdom

(51) INT CL[6]
G06K 5/00 , G07F 7/12

(52) UK CL (Edition N)
G4H HTG H1A H13D H14A H14B H14D
U1S S1727 S2132 S2271

(56) Documents Cited
EP 0014313 A1 EP 0007002 A1

(58) Field of Search
UK CL (Edition M) G4H HTG
INT CL[5] G06K , G07F

(54) Authorizing credit cards and other cards

(57) A card authorization method for use by a department store having a large number of cash registers (1) each with a card swipe facility, comprises employing a dedicated communications line (6) between a cash register network (1, 2, 3, 5) in the department store and the card authorization agency (7) to convey multiple communications in a format determined by the card authorization agency (7) and controlling the flow of communications between the electronic cash registers (1) and the dedicated communications line (6) by means of communications control means (4) employing a communications interface protocol.

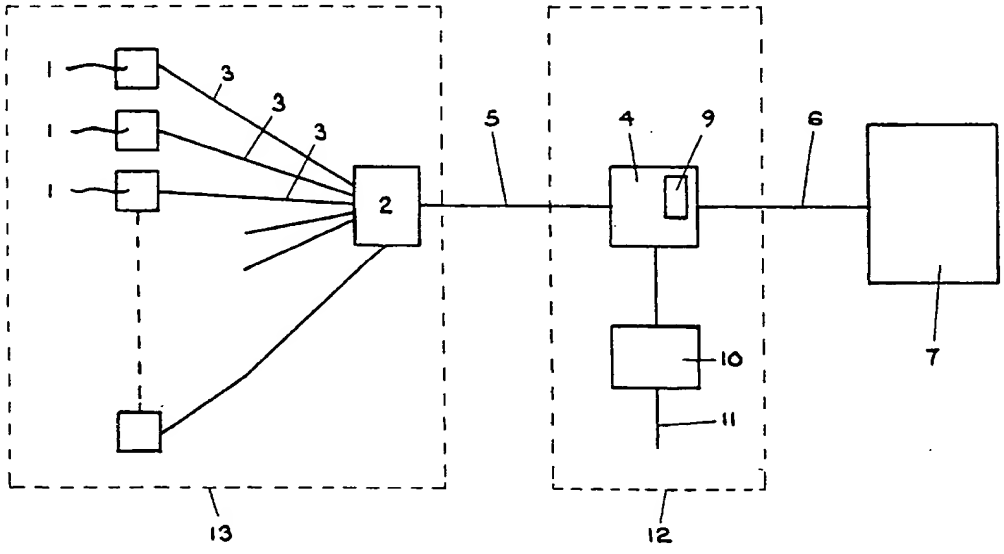

Fig 1

GB 2 281 648 A

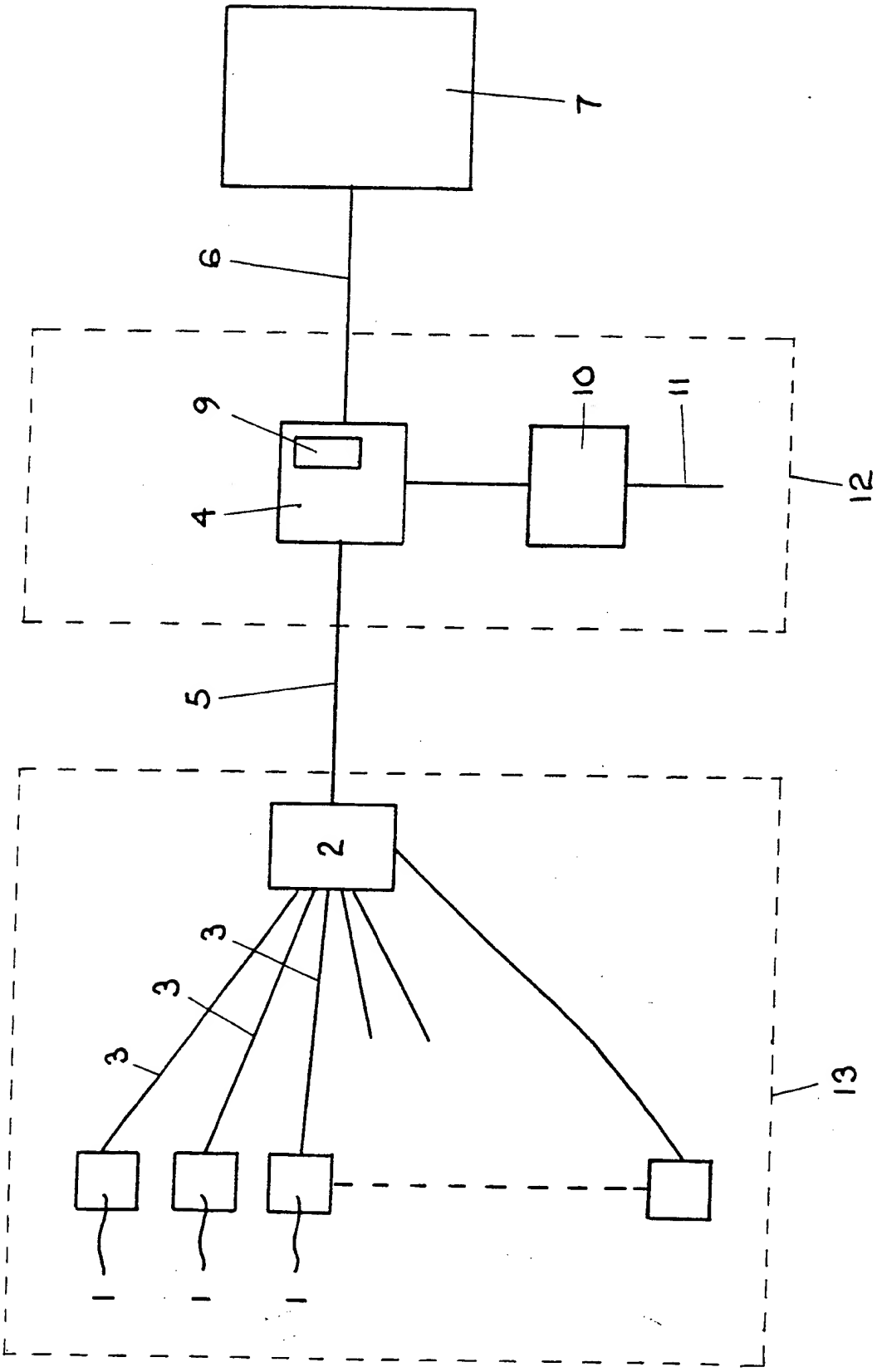

Fig 1

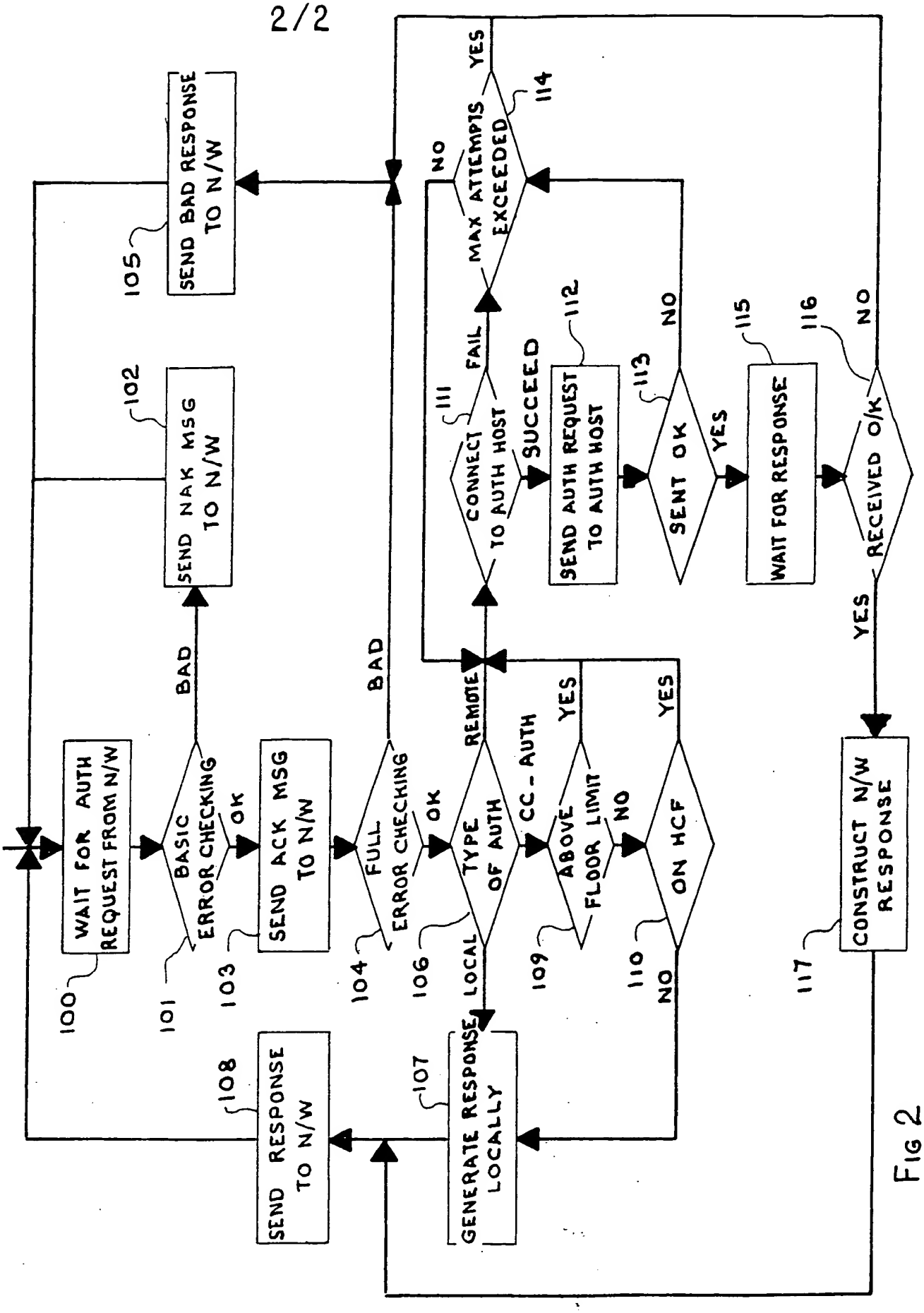
WAIT FOR AUTH REQUEST FROM N/W
100
BASIC ERROR CHECKING
101
BAD
OK
SEND NAK MSG TO N/W
102
SEND BAD RESPONSE TO N/W
105
SEND ACK MSG TO N/W
103
FULL ERROR CHECKING
104
BAD
OK
TYPE OF AUTH
106
REMOTE
LOCAL
CC - AUTH
ABOVE FLOOR LIMIT
109
YES
NO
ON HCF
110
YES
NO
GENERATE RESPONSE LOCALLY
107
SEND RESPONSE TO N/W
108
MAX ATTEMPTS EXCEEDED
114
YES
NO
CONNECT TO AUTH HOST
111
FAIL
SUCCEED
SEND AUTH REQUEST TO AUTH HOST
112
SENT OK
113
NO
YES
WAIT FOR RESPONSE
115
RECEIVED O/K
116
NO
YES
CONSTRUCT N/W RESPONSE
117

Fig 2

"Method and apparatus for authorising credit cards and other cards"

The present invention relates to a method and apparatus for use in authorization of credit cards and other cards, such as charge cards and debit cards, at points of sale.

The authorization of a card in a large department store has typically been carried out as follows. First, the shop assistant enters the value of the various items being purchased in a cash register. Then the customer presents the card. The shop assistant is now presented with the task of authorising the card, and this is done using a separate apparatus known as an EFT-POS device (Electronic Funds Transfer-Point of Sale device) supplied by the card authorization agency. Typically, there will be one EFT-POS device at each cash register. The card is swiped through a card reader forming part of the EFT-POS device, and the value of the transaction is keyed into a keyboard forming part of the EFT-POS device. The EFT-POS device then automatically dials up the card authorization agency through a modem and along the public telephone network, transmits the authorization query, and receives a response all in accordance with a format or protocol set by the card authorization agency. Typically, the response will

consist of authorization, or refusal to authorise, or an instruction to retain the card which may have been reported as stolen or missing.

The above described method and apparatus suffers from many disadvantages. The method and apparatus is time consuming, involving manual entry of the total shown in the cash register into the EFT-POS device. Communications difficulties are often experienced, for example, the telephone lines may be engaged. The customer experiences the irritation of waiting until a connection is made and a card authorized. Smaller transactions are not checked and the merchant must bear the risk and regularly incur small losses. Also, no record is kept and therefore no management information is available which identifies and distinguishes transactions carried out by card rather than cash. Finally, the merchant must pay a rental for each EFT-POS device to the bank which supplied the device.

More recently, a system has been available including an electronic cash register with a swipe facility and an EFT-POS device connected to the cash register. When the shop assistant has entered the value of the purchases in the cash register and the cash register has added up the total, if the customer presents a card, the shop assistant can swipe the card through the

cash register, and this information is transmitted to the EFT-POS device which automatically dials the card authorization agency and seeks authorization. The advantage of this arrangement is that there is no need to manually enter the total value of the transaction. Also, the cash register is able to distinguish between cash and credit transactions for the purposes of management information. However, the other disadvantages still remain.

An object of the present invention is to provide an improved method and apparatus for authorising use of cards.

The invention provides a card authorization method for use by a retail sales outlet having a plurality of electronic cash registers each having a card swipe facility, comprising

- conveying multiple card authorization requests between the retail sales outlet and the card authorization agency along a dedicated communications line between the two in accordance with a protocol determined by the card authorization agency
- and controlling the flow of card authorization communications between the electronic cash registers and the dedicated communications line by means of communication control means employing a communications

interface protocol.

The use of a dedicated communications line is much quicker and more efficient because the amount of data transmitted to and received from a card authorization agency for each authorization is very small, typically eighty bytes. In the prior art the time taken for dialling is actually much greater than the time taken for transmission and reception.

Preferably, the communications interface protocol employs a format which is condensed relative to the format used on the dedicated communications line.

This feature of the invention is based on the appreciation that whereas the format in which messages are sent to and received from the card authorization agency along the dedicated communications line is determined by the card authorization agency, a more condensed format used in the department store allows more messages to be stored, processed and queued for transmission.

The invention provides card authorization apparatus for use by a retail sales outlet having a plurality of electronic cash registers each having a card swipe facility associated therewith, in order to communicate

with a card authorization agency comprising

- a dedicated communications line from the retail outlet to the card authorization agency for conveying multiple card authorization communications between the two in accordance with a protocol determined by the card authorization agency

- and communications control means between the electronic cash registers and the dedicated communication line for controlling the flow of card authorization communications between them, the communication control means employing a communication interface protocol to allow communication between the electronic cash registers and the dedicated communications line.

The invention may be implemented in a retail sales outlet having a cash register network consisting of a plurality of electronic cash registers each having a card swipe facility associated therewith and a sales outlet management information computer, in order to communicate with a card authorization agency, by means of apparatus comprising

- a dedicated communications line from the retail sales outlet to the card authorization agency for conveying multiple card authorization communications between the two in accordance with a protocol determined by the card authorization agency

- and a communications control computer between the management information computer and the dedicated communications line for controlling the flow of card authorization communication between the electronic cash register via the management information computer to the dedicated communications line, the communication control computer employing a communication interface protocol to allow communication between the electronic cash registers and the dedicated communications line.

The invention may be implemented in a retail sales outlet having a plurality of electronic cash registers each having a card swipe facility associated therewith, in order to communicate with a card authorization agency, by means of apparatus comprising

- a dedicated communications line from the retail sales outlet to the card authorization agency for conveying multiple card authorization communications between the two in accordance with a protocol determined by the card authorization agency

- and a communications control computer connected between the electronic cash registers and the dedicated communications line for controlling the flow of card authorization communications between them, the communications control computer employing a communication interface protocol to allow communication between the electronic cash registers and the dedicated

communications line.

The invention will now be described more particularly with reference to the accompanying drawing which shows, by way of example only, one construction of apparatus according to the invention. In the drawings,

Fig. 1 is a network in accordance with the invention, and

Fig. 2 is a flow chart of the authorization process.

Referring to Fig. 1, there is illustrated communications apparatus generally designated by reference numeral 12 according to the invention for connecting a cash register network generally designated 13 with an authorization agency 7. The cash register network 13 comprises electronic cash registers 1, a management information computer 2 and communications lines 3 between each cash register 1 and the management information computer 2. Such cash register networks 13 are known to those skilled in the art. Each cash register 1 includes a card swipe facility.

The communications apparatus 12 comprises a card authorization computer 4, a communications line 5

between the two computers 2,4, and a dedicated communications line 6 to the card authorization agency 7.

The card authorization computer 4 includes a receiver 9 for receiving on a periodic basis, typically every few seconds, a signal updating the list of lost and stolen cards (the "hot card file").

The above description relates to just one card authorization agency 7. In practice, at a typical retail sales outlet, one, two or three popular cards will account for a very large proportion of all card transactions. These cards will be authorized via dedicated lines. In the case of less popular cards the card authorization computer 4 will make use of a modem 10 and a non-dedicated line 11, in the same manner as with a traditional card authorization system. The modem 10 and non-dedicated line 11 are also useful as back-up in the event of any failure of the dedicated line 6.

To explain the invention more fully, the various messages being transmitted about the network will be explained.

An electronic cash register 1 required to authorise a

card transmits to the management information computer 2 along communication line 3 a message which includes identification of the particular cash register 1, an indication that the message is a request for authorization, identification of the card, and the value of the proposed transaction. Only one transaction is handled at a time at a particular cash register 1, that is to say the shop assistant seeks authorization in respect of one card and the shop assistant and customer await the response before the shop assistant seeks authorization in respect of a second card.

The management information computer 2, on receiving messages from electronic cash registers 1, separates the card authorization requests from other messages and relays the card authorization requests to the card authorization computer 4 along communications line 5.

The card authorization computer 4 then transmits a message along dedicated communications line 6 to the card authorization agency, 7 again consisting of identification of the particular cash register 1, an indication that the message is a request for authorization, identification of the card, and the value of the proposed transaction.

If the card authorization agency 7 is a bank, the bank may authorize the use of the card and simultaneously credit the amount to the merchant. Similarly, where the customer is using a debit or charge card, the bank can instantaneously debit the customer's account.

The card authorization agency 7 determines its response in conventional manner and then transmits along dedicated communication line 6 to the card authorization computer 4 a message including the response to the request for authorization, the identification of the cash register, and possibly some text explaining the reasons for the response, for example, "expired card". Other messages are transmitted from the card authorization agency 7 to the card authorization computer 4 include a list of cards reported lost or stolen or promotional data.

The card authorization computer 4 in turn transmits along communication line 5 to the management information computer 2 a message including the response, identification of the cash register, and the printed text mentioned above. The card authorization computer 4 may also transmit other messages, including housekeeping messages such as the length of the queue for the dedicated communication line 6.

The management information computer 2 then transmits along the appropriate communication line 3 to the electronic cash register 1 a message consisting of the response and the text mentioned above. The management information computer 2 may also transmit to the electronic cash register the queuing information and other housekeeping matters mentioned above.

Fig. 2 is a flow chart of a subroutine of a computer programme which controls operation of card authorization computer 4. The subroutine is concerned with those operations carried out at the card authorization computer 4 which relate specifically to card authorization, and does not include other operations, for example the various housekeeping operations mentioned above.

Block 100 represents the card authorization computer 4 waiting for an authorization request from the network 1,2,3,5. On a request being received the subroutine moves to block 101 which checks the message received by the card authorization computer 4 from the network 1,2,3,5 for any basic errors. If a basic error is present, then the subroutine proceeds to block 102, which involves sending a message from the card authorization computer 4 to the network 1,2,3,5 indicating that the message is not acknowledged. If

the message is found to be in order, then the subroutine proceeds to block 103, which involves sending an acknowledgement message to the network 1,2,3,5. Block 104 represents a full check of the received message for errors. Again, if the full check reveals an error, then the subroutine proceeds to block 105 which involves sending to the network 1,2,3,5 an indication that the message is bad. If the message is found to be in order, then the subroutine proceeds to block 106 which identifies the type of authorization required.

If the authorization can be done in-house, for example, in the case of a department store card or if the transaction indicates that a local authorization is sufficient, the subroutine then proceeds to block 107, at which the response is generated within the department store. The subroutine then proceeds to block 108, which involves transmitting the response to the network 1,2,3,5. If the request for authorization is recognised as being one for which a local authorization is to be performed if certain criteria are met, then the subroutine proceeds to block 109, which involves checking whether the value of the transaction is above the credit limit for the particular card. If the answer is no, the subroutine then proceeds to block 110, to check whether the card

is on the "hot card" file. If the answer is no, then the subroutine proceeds to blocks 107 and 108.

If the authorization cannot be done in-house because the transaction does not comply with the criteria, or the transaction specifically indicates that an on-line transaction must be performed, then block 111 represents an attempt to connect the card authorization computer 4 to an external card authorization agency 7. If the attempt succeeds, the subroutine proceeds to block 112, which involves transmitting the authorization request to the card authorization agency 7.

Block 113 represents checking whether the message has been successfully transmitted to the card authorization agency. In the event that the message has not been successfully transmitted, the subroutine proceeds to block 114, which represents a check on the number of attempts made to send the message, and if the number has not been too great, then the subroutine proceeds back to block 111 and again attempts to transmit the message. However, if the number of attempts already made exceeds the maximum permitted number, then the subroutine proceeds back to block 115, and indicates that it has not been possible to send the message.

At block 113, if the message is successfully sent, then the subroutine proceeds to block 115, which represents waiting for a response from the card authorization agency 7, and then proceeds to block 116 which involves determining whether a response has been received. In the event that block 116 determines that a proper response has not been received, the subroutine then proceeds to block 105. If at block 116 a determination is made that a proper response has been received, then the subroutine proceeds to block 117, which involves the card authorization computer 4 constructing a response in a format suitable to be transmitted to the network and onwards to the particular cash register.

Timing

Turning now to the time taken for one authorization request, assuming no other authorization request were present, the time taken would be as follows:

a) card authorization computer 4 receives message from management information computer 2, recognises this message as a request for authorization and sends an acknowledgement 0.1 s

b) card authorization computer 4 analyzes the message, reformats the message (see below) and transmits

	the message to the card authorization agency 7 along dedicated line 6	0.5 s
c)	card authorization agency 7 receives message, determines response, and response is conveyed along dedicated line 6	0.5 s
d)	card authorization computer 4 analyses response, reformats response (see below) and transmits response to management information computer 2	0.3 s
	Total	1.4 s

In both (b) and (c) above the transmission time on the dedicated line 6 represents only approximately one tenth of the time mentioned, with most of the time taken up with the analysis and reformatting.

The dedicated communications line makes use of standard network technology, for example X.25 technology, which is a CCITT standard, and which is well known to those skilled in the art. For a department store with between one and two hundred electronic cash registers, a dedicated communications line capable of handling up to sixty four messages in parallel has been found to be

sufficient. Message queuing is virtually eliminated.

In the embodiment described above, with between one and two hundred cash registers, while the time taken for authorization of one transaction, if it were the only one present, would be 1.4 seconds, a typical actual response time is 4 seconds, and the target time is less than 7 seconds.

The embodiment described above relates to a retail outlet already provided with a management information computer 2. In the case of a store with electronic cash registers 1 not linked to a management information computer 2, then the cash registers 1 may be linked directly to a card authorization computer 4, which advantageously may also perform the functions of a management information computer 2.

The format in which communications take place along the dedicated line 6 is set by the card authorization agency 7. Typically, formats used by card authorization agencies 7 tend to be rather long and not economical of computer storage space and transmission time. Heretofore there has been no requirement for brief messages with a short transmission time, given that each electronic cash register 1 made use of time consuming dialling, with the dialling time being much

greater than the transmission time.

If however such a long format were used throughout the network, and in particular in the card authorization computer 4, then the long processing time at the computer 4 would limit the number of transactions which may be handled. Instead, in accordance with the invention, messages which appear in one format at the electronic cash register 1 and in another format on the dedicated line 6 pass through an intermediate format, called the communication interface protocol, which will be described in more detail below, and which is very condensed and economical in terms of the number of bytes of information required for a message, thereby allowing messages to be analyzed, stored and queued at the computer authorization computer 4, using as little processing time as possible, bearing in mind that with the elimination of dialling time and modem time the limiting factor in reducing time is the processing time.

In the first embodiment described above the communication interface protocol is used between the electronic cash registers 1 and management information computer 2 (for card authorization messages only), with the traditional format being used for all other messages. To allow the electronic cash registers 1 to

handle the communication interface protocol the original software in the cash registers 1 is substituted by modified software. All communications between the management information computer 2 and the card authorization computer 4 employ the communications interface protocol.

In the second embodiment described above the communication interface protocol is used between the electronic cash registers 1 and the card authorization computer 4.

Communications Interface Protocol

This protocol is based on the idea of messages consisting of a code which indicates the general family of commands to which the request applies (e.g. inquiry, status, command, etc.) and a subcode indicating the particular command within that family. Each code/subcode pair may also have a set of command specific data associated with it.

All messages between the card authorization computer 4 and the network 1,2,3,5 should be of the form:
<STX<>CODE><SUBCODE><MSGID>[<COMMAND SPECIFIC DATA>]<ETX>[<LRC>]

where <STX> is one byte long and represents the start

of the message, <CODE> is two bytes long and indicates the general family of commands, <SUBCODE> is two bytes long and indicates the particular command within the family, <MSGID> is four bytes long and indicates the identity of the sender, <COMMAND SPECIFIC DATA> is of a variable length and indicates data such as a card number in relation to which a command is to be performed or the value of a transaction, <ETX> is one byte long and represents the end of the message, and <LRC> represents an optional error check, indicating whether the message has been correctly received.

All allowed combinations of codes and subcodes are discussed below.

Every message sent to the card authorization computer 4 contains the four byte message id - to avoid repetition the presence of this message id is assumed in the discussion below, and is not mentioned explicitly. Below is given a comprehensive listing of all software commands, including not only card authorization commands but also the housekeeping commands. The following conventions apply:

<NNNNNN>	represents a number
<12 BYTES DATA>	represents the amount field in pence
<TTTT>	represents the time of day in HH:MM

<II> represents the Issuer ID (e.g. AMEX - 02, VISA - 03, etc.)

<ACSC> is a three character code indicating whether the card was swiped, manually entered, authorised locally or by a card authorization agency.

The INQUIRY family of commands

A code of "01" indicates that the request is for one of the commands in the inquiry family of commands. These commands allow the management information computer 2 to obtain information held on the card authorization computer 4, and this family of commands relates to diagnostics and maintenance. The commands in this family are:

1) GET_SW_REVISION:

A subcode of "01" will invoke the GET_SW_REVISION command, which returns a response indicating the current version of the software running on the card authorization computer 4.

2) QUEUE_LENGTH:

A subcode of "02" will invoke the QUEUE_LENGTH command. This returns a response indicating the number of pending messages in the card authorization computer 4 queue.

3) CURRENT_STATE:

A subcode of "03" will invoke the CURRENT_STATE command. This returns a response indicating the current communications state (e.g. dialling, transmitting, receiving, hung up) of the card authorization computer 4.

4) AUTH_COUNT:

A subcode of "04" will invoke the AUTH_COUNT command. The response, which may be used for statistical purposes, contains the total number of authorizations transmitted through the card authorization computer 4 since the last inquiry.

5) II_AUTH_COUNT:

A subcode of "05", and command specific data containing a valid issuer id (a two digit code), will invoke the II_AUTH_COUNT command. The response contains the total number of authorizations for that card issuer since the last inquiry.

6) NOT_AUTH_COUNT:

A subcode of "06" will invoke the NOT_AUTH_COUNT command. The response contains the total number of referrals (authorization refusals) since the last inquiry.

7) MONEY_AUTH_COUNT:

A subcode of "07" will invoke the MONEY_AUTH_COUNT

command. The response contains the total value of authorised transactions since the last inquiry.

8) II_MONEY_AMOUNT_AUTH:

A subcode of "08", and command specific data containing a valid issuer id, will invoke the II_MONEY_AMOUNT_AUTH command. The response contains the total value of authorised transactions for that card issuer since the last inquiry.

The STATUS family of commands

A code of "02" indicates that the request is for one of the commands in the status family of commands. These commands allow the management information computer 2 to set certain characteristics of the card authorization computer 4, that is to say to initialise or reset the system. The commands in this family are:

1) PUT_SW_REVISION:

A subcode of "01", followed by command specific data containing a text string of maximum forty characters, will invoke the PUT_SW_REVISION command. This sets the current software revision of the card authorization computer 4 to be the text string passed in the message, and this text string is then available as a response to a query as to which version of the software is in use.

2) PUT_QUEUE_LENGTH:

A subcode of "02", followed by command specific data containing a <NNNNNN> field, will invoke the PUT_QUEUE_LENGTH command. This sets the current queue length to be the value contained in the <NNNNNN> field, usually zero for initialisation purposes.

3) PUT_CURRENT_STATE:

A subcode of "03", followed by command specific data containing a text string of maximum forty characters, will invoke the PUT_CURRENT_STATE command. This sets the current communications state of the card authorization computer 4 to be the text string passed in the message, for example "HUNG UP", for initialisation purposes.

4) PUT_AUTH_COUNT:

A subcode of "04", followed by command specific data containing a <NNNNNN> field, will invoke the PUT_AUTH_COUNT command. This command sets the current authorization count (the total number of authorizations since the last inquiry) to be <NNNNNN>.

5) PUT_II_AUTH_COUNT:

A subcode of "05", followed by command specific data containing a valid issuer id <II>, and a number <NNNNNN>, will invoke the PUT_II_AUTH_COUNT command. This command sets the authorization count for issuer <II> to be

<NNNNNN>, typically zero at the beginning of the day, week, month, etc.

6) PUT_NOT_AUTH_COUNT:

A subcode of "06", followed by command specific data containing a <NNNNNN> field, will invoke the PUT_NOT_AUTH_COUNT command. This command sets the referral count (the total number of referrals since the last inquiry) to be <NNNNNN>, typically zero at the beginning of the day.

7) PUT_MONEY_AMOUNT_AUTH:

A subcode of "07", followed by command specific data containing a <12 BYTE DATA> amount field, will invoke the PUT_MONEY_AMOUNT_AUTH command. This command sets the authorised amount (the total value of authorizations since the last inquiry) to be <12 BYTE DATA>.

8) PUT_II_MONEY_AMOUNT_AUTH:

A subcode of "08", followed by command specific data containing a <12 BYTE DATA> amount field and a <II> issuer id field, will invoke the PUT_II_MONEY_AMOUNT_AUTH command. This command sets the authorised amount for the issuer <II> (the total value of authorizations for that issuer since the last inquiry) to be <12 BYTE DATA>.

The COMMAND family of commands

A code of "09" indicates that the request is for one of the commands in the command family. These commands are most directly concerned with the authorization of credit cards.

1) LRC_OFF:

A subcode of "00" will invoke the LRC_OFF command. This indicates to the card authorization computer that no LRC (longitudinal redundancy code) character is to be expected on incoming messages, including this one. This command may be used during testing of the network.

2) LRC_ON:

A subcode of "01" will invoke the LRC_ON command. This indicates that for a message to be correct it must contain an LRC. The current message is excluded. Typically, this command may be used during testing of the network. Normally, an error message is not required in use when a short communication line is being employed, but is required when a long communication line is required.

3) CHANGE_BAUDRATE:

A subcode of "03", followed by command specific data containing a <NNNNNN> field, will invoke the CHANGE_BAUDRATE command. After this message, the serial speed will be changed to <NNNNNN>. Typically, this

command may be used during testing of the network.

4) ECHO_ON:

A subcode of "04" invokes the ECHO_ON command. This indicates to the card authorization computer 4 that all characters are to be echoed back to the network. The current message is excluded. This command is used during testing.

5) ECHO_OFF:

A subcode of "05" invokes the ECHO_OFF command. This indicates to the card authorization computer 4 that after the current message has been processed, no further characters are to be echoed to the network. This command is used during testing.

6) TEST-LINK

A subcode of "06" invokes the TEST_LINK command. If the card authorization computer 4 correctly receives and interprets this message, a good packet message is sent to the network. Otherwise a bad packet message is sent. This command is used regularly.

7) ISSUE_TEST

A subcode of "07", followed by command specific data containing an issuer id, invokes the ISSUE-TEST command. The card authorization computer 4 will issue a test to

the authorization host specified for that particular issuer. The response message contains a result code indicating success or failure.

8) AUTHORISE_CC:

A subcode of "10", followed by command specific data containing an <ACSC> code, track 2 data, and an amount field will invoke the AUTHORISE_CC command. This command checks for the presence of the card number in the hot card file (HCF). If the card number is present then an on-line authorization is performed. Otherwise the amount field is checked to see if the amount is over the transaction value floor limit specified for the card issuer in question. If the amount is over the floor limit, an on-line authorization is performed. Otherwise a local authorization is performed. The exact flow involved in this process is illustrated in Fig. 2.

The response message to the network contains a response code indicating the success or failure of the authorization, a text field containing an English language equivalent to the response code, and an authorization code, if appropriate.

9) AUTHORISE_LOCAL:

A subcode of "11", followed by command specific data containing an <ACSC> code, track 2 data, and an amount

field will invoke the AUTHORISE_LOCAL command. In this case the merchant is taking responsibility for the authorization, which is always performed locally. The card is checked against the HCF. If the card appears in the HCF, authorization fails, if not authorization succeeds. The exact flow involved in this process is illustrated in Fig. 2.

The response message from the card authorization computer 4, and without seeking authorization from the card authorization agency 7 contains a response code indicating the success or failure of the authorization, a text field containing an English language equivalent to the response code, and an authorization code, if appropriate.

10) AUTHORISE_REMOTE:

A subcode of "12", followed by command specific data containing an <ACSC> code, track 2 data, and an amount field will invoke the AUTHORISE-REMOTE command. In this case authorization is always performed on-line, even if the card does not appear on the HCF, and the amount is under the transaction value floor limit. This command is used if the shop assistant is suspicious of the bona fides of the person presenting the card. The exact flow involved in this process is illustrated in Fig. 2.

The response message to the network contains a response code indicating the success or failure of the authorization, a text field containing an English language equivalent to the response code, and an authorization code, if appropriate.

11) AUTHORISE_DC:

A subcode of "20", followed by command specific data containing an <ACSC> code, track 2 data (e.g. expiry data, security codes), track 3 data (e.g. name, address), and an amount field will invoke the AUTHORISE_DC command. This command, involving a request for authorization of a debit card, and including confidential information, namely the Personal Identification Number (PIN) of the user, is sent direct to the bank without reformatting to protect the identity of the user.

The response message to the network contains a response code indicating the success or failure of the authorization, a text field containing an English language equivalent to the response code, and an authorization code, if appropriate.

12) BATCH_NOW:

A subcode of "30", followed by command specific data containing the supervisor password, will invoke the BATCH_NOW command. This instructs the card authorization

computer 4 to immediately batch all the captured transactions to the correct data capture host, for example, sending details of a weeks transactions to a bank for settlement.

The response message to the network contains a text field which displays the response from the data capture host, and a response code indicating the success or failure of the batching attempt.

13) BATCH_AT_TIME:

A subcode of "31", followed by command specific data containing the supervisor password and a <TTTT> field, will invoke the BATCH_AT_TIME command. This instructs the card authorization computer 4 to batch all the captured transactions to the correct data capture host at the time specified by the <TTTT> field, for example, overnight.

The response message to the network is a confirmation that the message was correctly received.

14) CLEAR_HCF:

A subcode of "50", followed by command specific data containing the supervisor password, will invoke the CLEAR_HCF command. This instructs the card authorization computer 4 to delete all entries from the resident hot

card file, for initialisation purposes.

The response message to the network is a confirmation that the resident hot card file is now empty.

15) DUMP_HCF:

A subcode of "51", followed by command specific data containing a four byte code indicating packet size, will invoke the DUMP-HCF command. This instructs the card authorization computer 4 to dump the resident hot card file to the network, in packets each of which contain the specified number of card numbers (given by the packet size parameter), for example, one hundred at a time, followed by an acknowledgement, before sending the next packet of one hundred.

Each packet from the card authorization computer 4 to the network contains the packet number, the total number of packets required to dump the hot card file, the number of card numbers in this particular packet, followed by a list of the individual card numbers.

16) INIT_HCF:

A subcode of "52", followed by command specific data containing a four byte code indicating packet size, will invoke the INIT_HCF command. This instructs the card authorization computer 4 that a hot card file is going to

be received by the card authorization computer 4 from the management information computer 2.

When the card authorization computer 4 acknowledges that it is ready to receive this hot card file, packets are received from the network. Each packet to the card authorization computer 4 from the management information computer 2 contains the packet number, the total number of packets required to receive the hot card file, the number of card numbers in this particular packet, followed by a list of the individual card numbers. When the file has been downloaded it becomes the resident hot card file.

17) ADD_CARD_NUMBER:
A subcode of "53", followed by command specific data containing a card number, will invoke the ADD_CARD_NUMBER command. This instructs the card authorization computer 4 to add the card number to the resident hot card file.

The response to the network is an acknowledgement that the addition has been successful.

18) DELETE_CARD_NUMBER:
A subcode of "54", followed by command specific data containing a card number, will invoke the DELETE_CARD_NUMBER command. This instructs the card

authorization computer 4 to delete the card number from the resident hot card file.

The response to the network is an acknowledgement that the deletion has been successful.

19) CARD_NUMBER_PRESENT:

A subcode of "55", followed by command specific data containing a card number will invoke the CARD_NUMBER_PRESENT command. This instructs the card authorization computer 4 to check whether the card number is present in the resident hot card file, this is a diagnostic request and is not a request for authorization.

The response to the network contains a response code indicating whether the card number was detected or not.

20) CANCEL_ALL:

A subcode of "90" will invoke the CANCEL_ALL command. This instructs the card authorization computer 4 to cancel all outstanding requests, if some untoward event takes place.

The response to the network is an acknowledgement that the cancel has been successful.

21) RESET_ALL:

A subcode of "91" will invoke the RESET_ALL command. This instructs the card authorization computer 4 to cancel all outstanding requests, and reset itself before accepting any further requests.

The response to the network is an acknowledgement that the reset has been successful.

The UNPROMPTED STATUS family of commands

While with all the previous commands the card authorization computer 4 has passively reacted to requests coming from the network, it is also capable of issuing unprompted messages to the network. The UNPROMPTED STATUS family is identified by a code of "05". The subcode "00" indicates an unprompted status message issued by the card authorization computer 4. This message also contains a two byte status code, indicating the current state of processing on the card authorization computer 4 as well as a maximum 40 byte text field giving an English language version of this status code. These messages can be sent at regular intervals without prompting from the card authorization computer 4 to the management information computer 2. Examples of such status messages are:

DIALLING

NO ANSWER

NO CARRIED

CONNECTED

SENDING DATA

RECEIVING DATA etc.

The UNPROMPTED INQUIRY family of commands

As well as being able to send unprompted status messages to the network, the card authorization computer 4 is also capable of issuing an unprompted inquiry message to the network. The UNPROMPTED ENQUIRY family is identified by a code of "06". A subcode of "00" indicates an unprompted inquiry issued by the card authorization computer 4.

The card authorization computer 4 will wait 30 seconds for an acknowledgement from the network. If it is not received then the card authorization computer 4 assumes that there is a communications failure with the network.

It will of course be appreciated that the invention is not limited to the specific details described herein which are given by way of example only and that various modifications and alterations are possible.

CLAIMS

1. A card authorization method for use by a retail sales outlet having a plurality of electronic cash registers each having a card swipe facility, comprising

- conveying multiple card authorization requests between the retail sales outlet and the card authorization agency along a dedicated communications line between the two in accordance with a protocol determined by the card authorization agency

- and controlling the flow of card authorization communications between the electronic cash registers and the dedicated communications line by means of communication control means employing a communications interface protocol.

2. A method according to Claim 1 in which the communications interface protocol employs a format which is condensed relative to the format used on the dedicated communications line.

3. A card authorization method for use by a retail sales outlet having a plurality of electronic cash registers each having a card swipe facility, the card authorization method being substantially as described herein with reference to and as illustrated in the accompanying drawings.

4. Card authorization apparatus for use by a retail sales outlet having a plurality of electronic cash registers each having a card swipe facility associated therewith, in order to communicate with a card authorization agency comprising

- a dedicated communications line from the retail outlet to the card authorization agency for conveying multiple card authorization communications between the two in accordance with a protocol determined by the card authorization agency

- and communications control means between the electronic cash registers and the dedicated communication line for controlling the flow of card authorization communications between them, the communication control means employing a communication interface protocol to allow communication between the electronic cash registers and the dedicated communications line.

5. Card authorization apparatus for use in a retail sales outlet having a cash register network consisting of a plurality of electronic cash registers each having a card swipe facility associated therewith and a sales outlet management information computer, in order to communicate with a card authorization agency, comprising

- a dedicated communications line from the retail

sales outlet to the card authorization agency for conveying multiple card authorization communications between the two in accordance with a protocol determined by the card authorization agency

- and a communications control computer between the management information computer and the dedicated communications line for controlling the flow of card authorization communication between the electronic cash register via the management information computer to the dedicated communications line, the communication control computer employing a communication interface protocol to allow communication between the electronic cash registers and the dedicated communications line.

6. Card authorization apparatus for use in a retail sales outlet having a plurality of electronic cash registers each having a card swipe facility associated therewith, in order to communicate with a card authorization agency, comprising

- a dedicated communications line from the retail sales outlet to the card authorization agency for conveying multiple card authorization communications between the two in accordance with a protocol determined by the card authorization agency

- and a communications control computer connected between the electronic cash registers and the dedicated communications line for controlling the flow of card

authorization communications between them, the communications control computer employing a communication interface protocol to allow communication between the electronic cash registers and the dedicated communications line.

7. Card authorization apparatus for use by a retail sales outlet having a plurality of electronic cash registers each having a card swipe facility associated therewith, in order to communicate with a card authorization agency, the card authorization apparatus being substantially as described herein with reference to and as illustrated in the accompanying drawings.

Patents Act 1977
Examiner's report to the Comptroller under Section 17
(T Search report) -40-

Application number
GB 9417777.1

Relevant Technical Fields

(i) UK Cl (Ed.M) G4H (HTG)

(ii) Int Cl (Ed.5) G06K, G07F

Search Examiner
M J DAVIS

Date of completion of Search
6 OCTOBER 1994

Databases (see below)
(i) UK Patent Office collections of GB, EP, WO and US patent specifications.

(ii)

Documents considered relevant following a search in respect of Claims :-
1 TO 7

Categories of documents

X: Document indicating lack of novelty or of inventive step.

Y: Document indicating lack of inventive step if combined with one or more other documents of the same category.

A: Document indicating technological background and/or state of the art.

P: Document published on or after the declared priority date but before the filing date of the present application.

E: Patent document published on or after, but with priority date earlier than, the filing date of the present application.

&: Member of the same patent family; corresponding document.

Category	Identity of document and relevant passages		Relevant to claim(s)
X	EP 0014313 A	(IBM) for example pages 14 to 25, 46 to 56	1, 4 to 6 at least
X	EP 0007002 A1	(IBM) whole document	1, 4 to 6 at least

Databases: The UK Patent Office database comprises classified collections of GB, EP, WO and US patent specifications as outlined periodically in the Official Journal (Patents). The on-line databases considered for search are also listed periodically in the Official Journal (Patents).